

FortiClient iOS - User Guide

VERSION 5.4.0

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



May 2, 2016

FortiClient iOS 5.4.0 User Guide

04-540-368848-20160502

TABLE OF CONTENTS

Change Log	4
Introduction	5
FortiClient (iOS) Features	5
Supported Platforms	5
Initial Configuration	6
Running FortiClient iOS	6
Mobileconfig Profile	9
Web Filtering	11
FortiHeartBeat	14
Logs	17

Change Log

Date	Change Description
2016-05-02	Initial Release.
2016-05-13	Added SSL VPN configuration note to the Introduction.

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This guide describes how to install and set up FortiClient iOS for the first time.

FortiClient (iOS) Features

Feature	Description
SSL VPN (Tunnel Mode)	SSL VPN in Tunnel Mode supports the following: <ul style="list-style-type: none">• IPv4 and IPv6• Full tunnel & split tunnel (IP and subnet based)• SSL realm, custom DNS server, DNS suffix• Username & password authentication• PKI user with a personal certificate, FortiToken & Client Certificate
Web Filter	All browser traffic is supported.
FortiHeartBeat	Connect to FortiGate and FortiClient EMS for central management.



In order to use the SSL DNS server for split tunnel, the DNS suffix needs to be configured on the FortiGate side.

Supported Platforms

FortiClient iOS is supported by iOS v9.0.0 and higher.

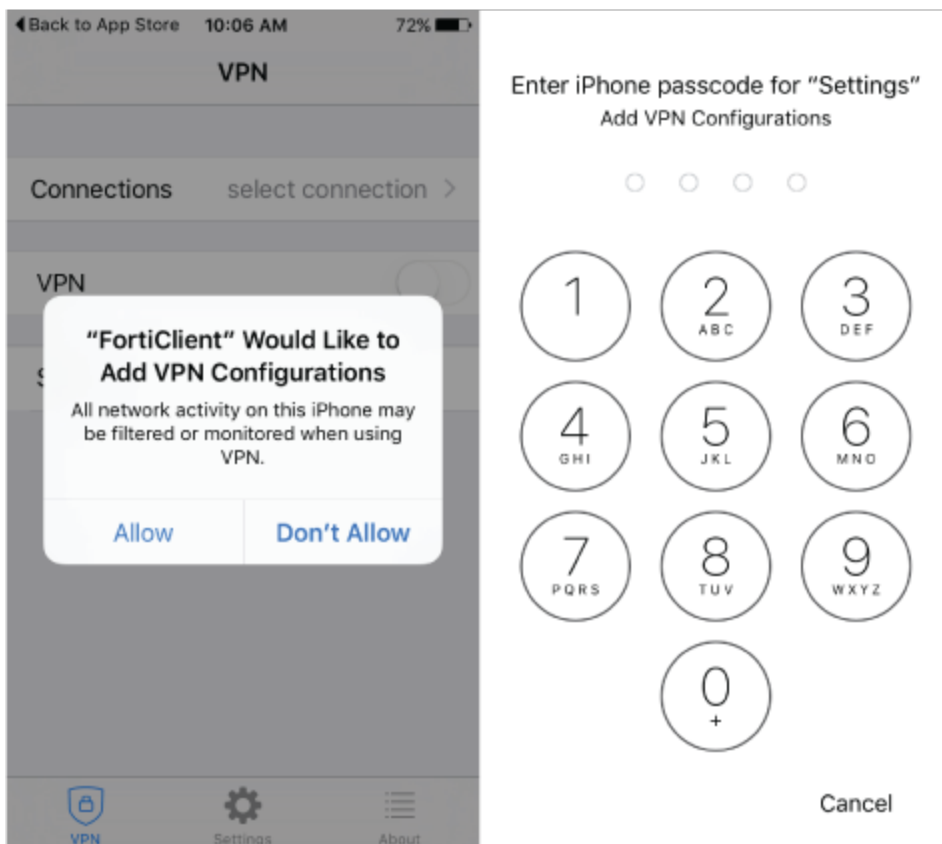
Initial Configuration

Running FortiClient iOS

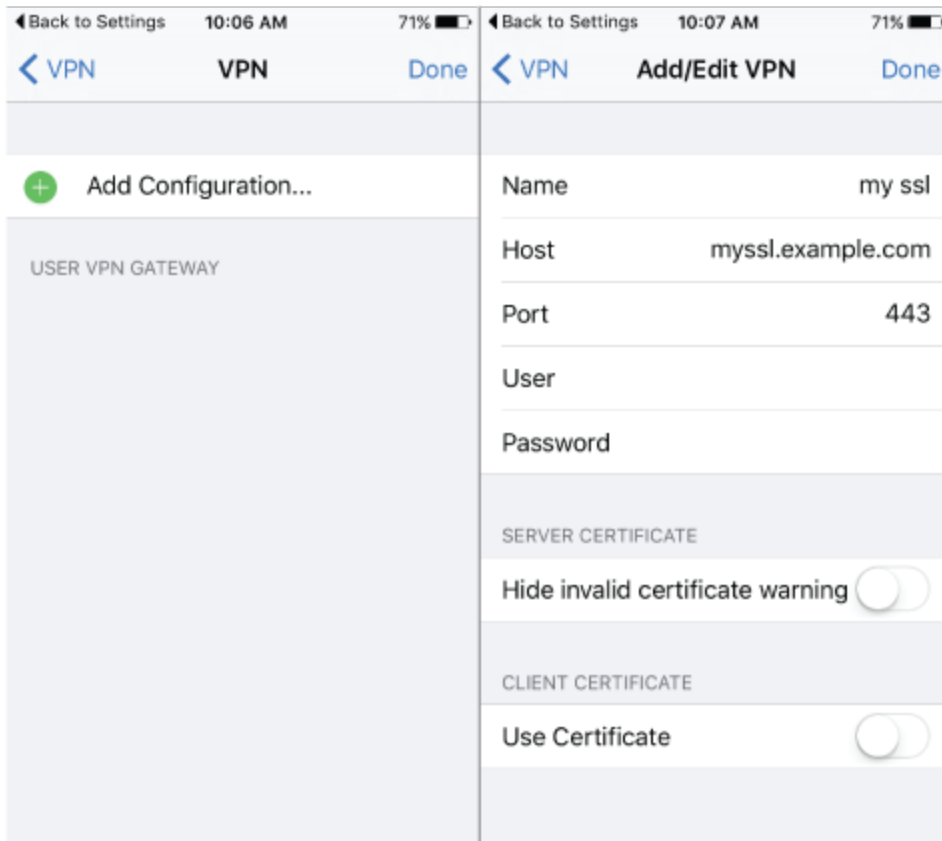
After downloading the FortiClient installer and running the application for the first time, a request to add a VPN configuration is sent.

To add a VPN Connection:

1. In the *Add VPN Configurations* pop up window, tap *Allow* and enter your passcode.



2. Tap the *VPN* icon at the bottom of the screen to switch to VPN page.
3. Tap *Add Configuration* and configure the following:



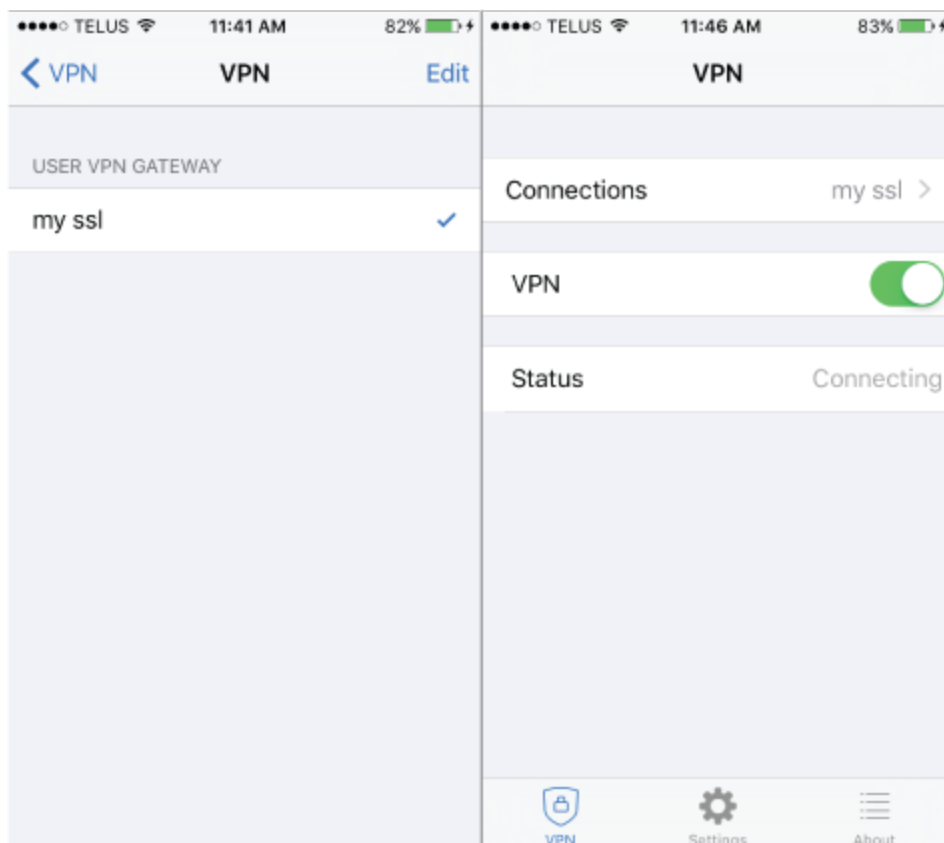
4. Tap *Done* twice.



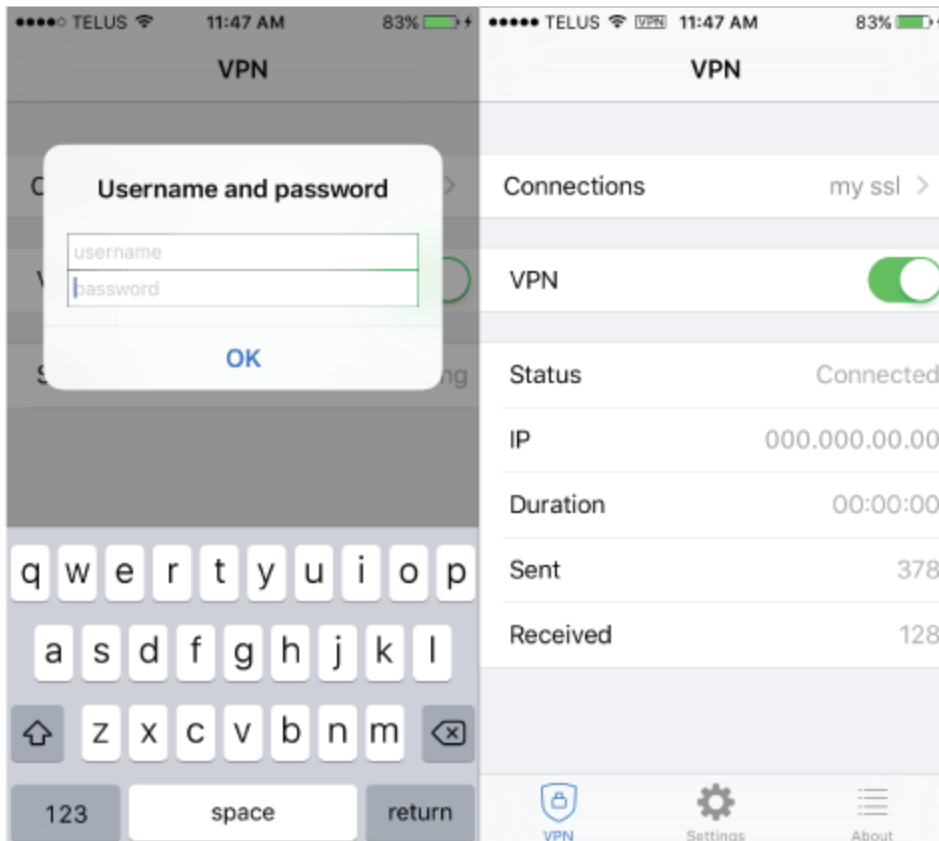
The Name, Host and Port fields are required, but User and Password, Hide invalid certificate warning, User Certificate are optional.

To enable a VPN connection:

1. Tap a *VPN connection*.
A check mark will appear beside the VPN connection to indicate it was selected.
2. Tap the < button.
3. Swipe right to enable the VPN connection.



4. If the user and password are not already configured, enter the *username and passcode* in the pop up window.



5. Tap **OK**.

When it is connected, the tunnel interface IP, duration, bytes sent and received information will be displayed.

To disable a VPN connection:

1. Select the VPN connection.
2. Swipe left to disable the VPN connection.

To edit or delete a VPN connection:

1. Select a VPN connection.
2. Tap *Edit* or *Delete*.
3. Tap *Done* twice.

Mobileconfig Profile

In order to enable Web Filtering, the iOS device will need to be supervised and a Mobileconfig Profile with Content Filter will need to be installed on the device.

Requirements:

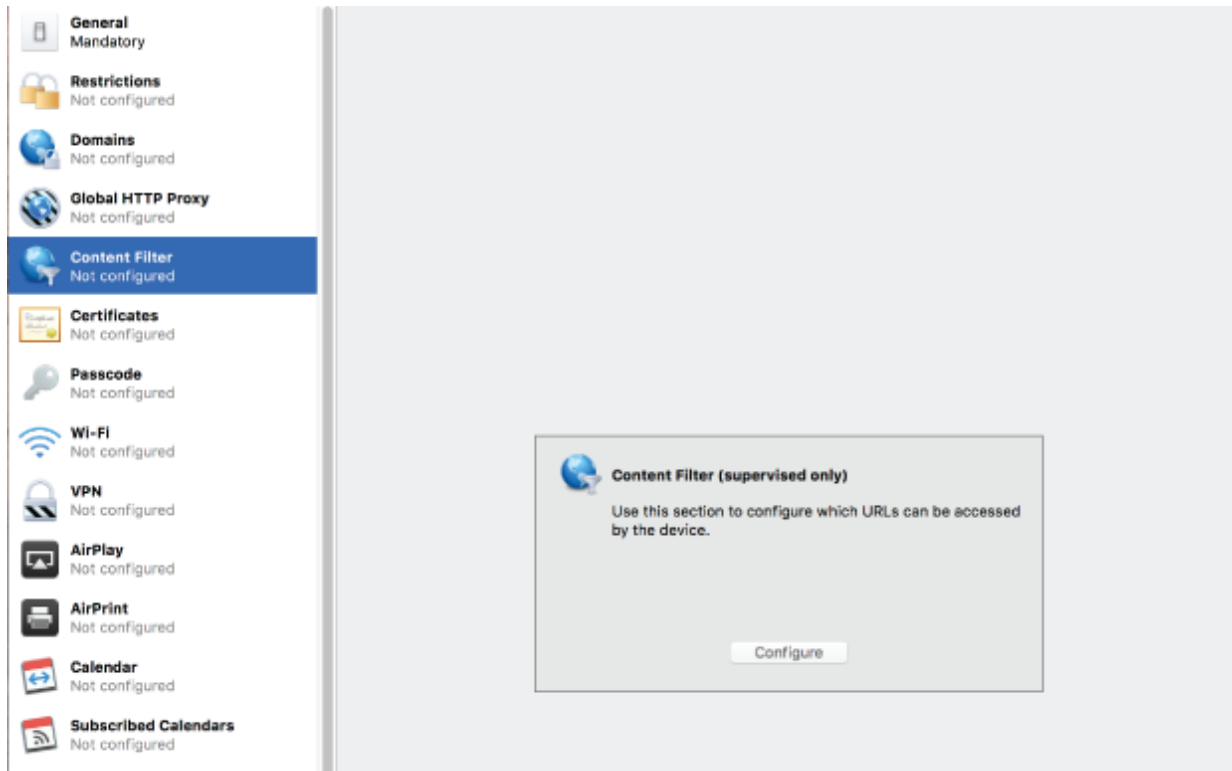
1. Apple Configurator 2 installed
2. iOS devices are supervised

How to supervise your iOS devices:

Instructions on how to supervise your iOS devices can be found on the [Apple Configurator 2 Help](#) website.

How to create a mobileconfig profile for FortiClient Web Filtering:

1. Launch *Apple Configurator 2*.
2. Go to *File > New Profile*.
3. Enter a *Name* for the profile.
4. Select *Content Filter* from the left panel.



5. Click *Configure*.
6. Select *Third Party App* from the *Filter Type* drop down.

7. Configure the following:

Filter Name	FortiClient
Identifier	com.fortinet.forticlient
Service Address	fgd1.fortigate.com
Organization	Fortinet, Inc.
User Name	TestUser
Certificate	Not applicable Certificate payload is configured.
Filter WebKit Traffic	Check the Filter WebKit Traffic box.
Custom Data	N/A..

9. Click *Save*.

Web Filtering

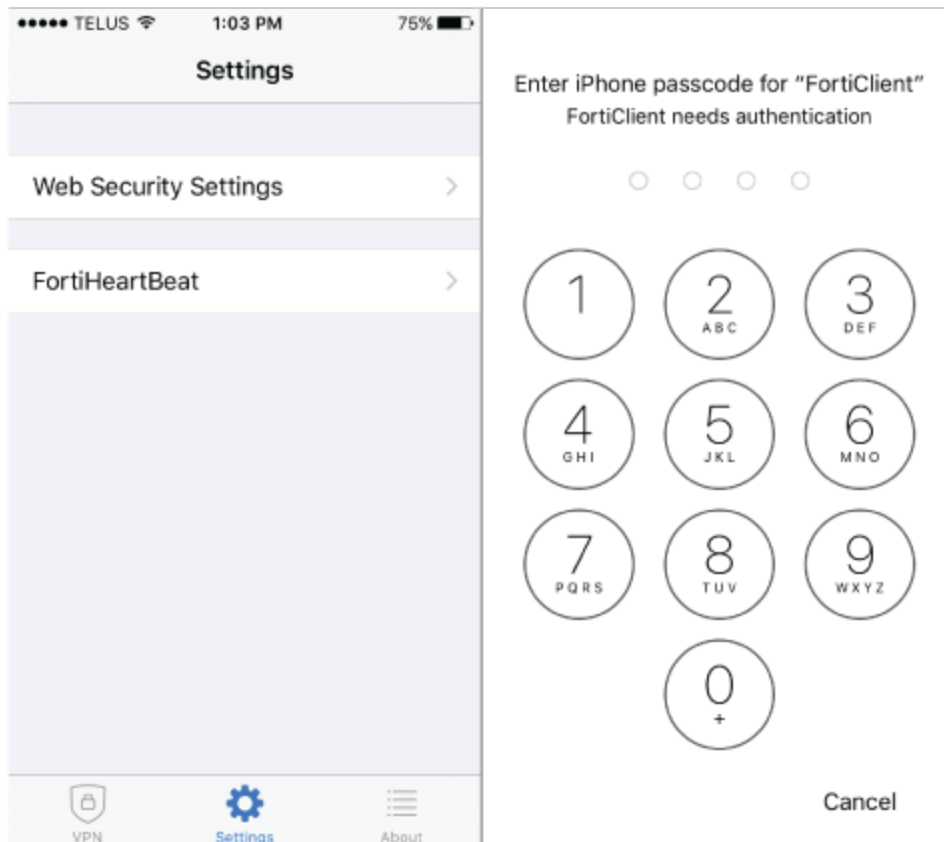


Web Filtering is disabled by default.

In order to enable Web Filtering, the iOS device will need to be supervised and a Mobileconfig Profile with Content Filter will need to be installed on the device. See [Create a Mobileconfig Profile](#).

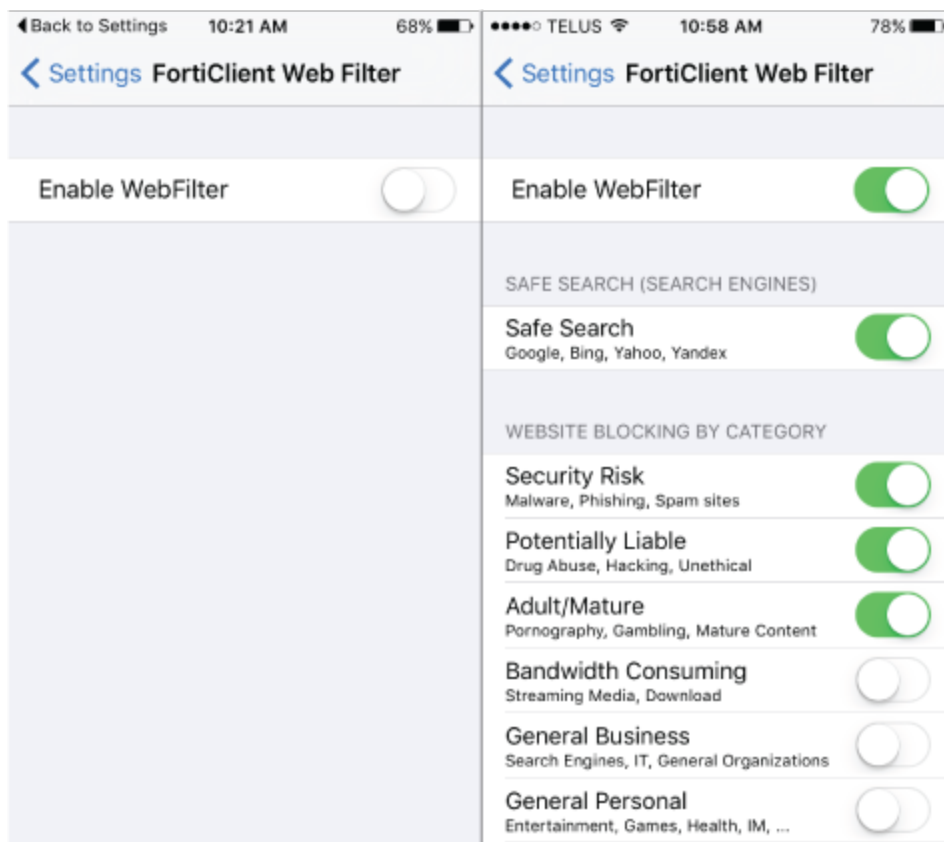
To configure the Web Filtering settings:

1. Tap *Settings* at the bottom of the screen.



2. Tap *Web Security Settings*.
3. Enter the passcode in the *FortiClient Authentication* pop up window.
4. Enable the *Web Filter* by swiping right.

5. Configure the *Website Blocking by Categories* to suit requirements.

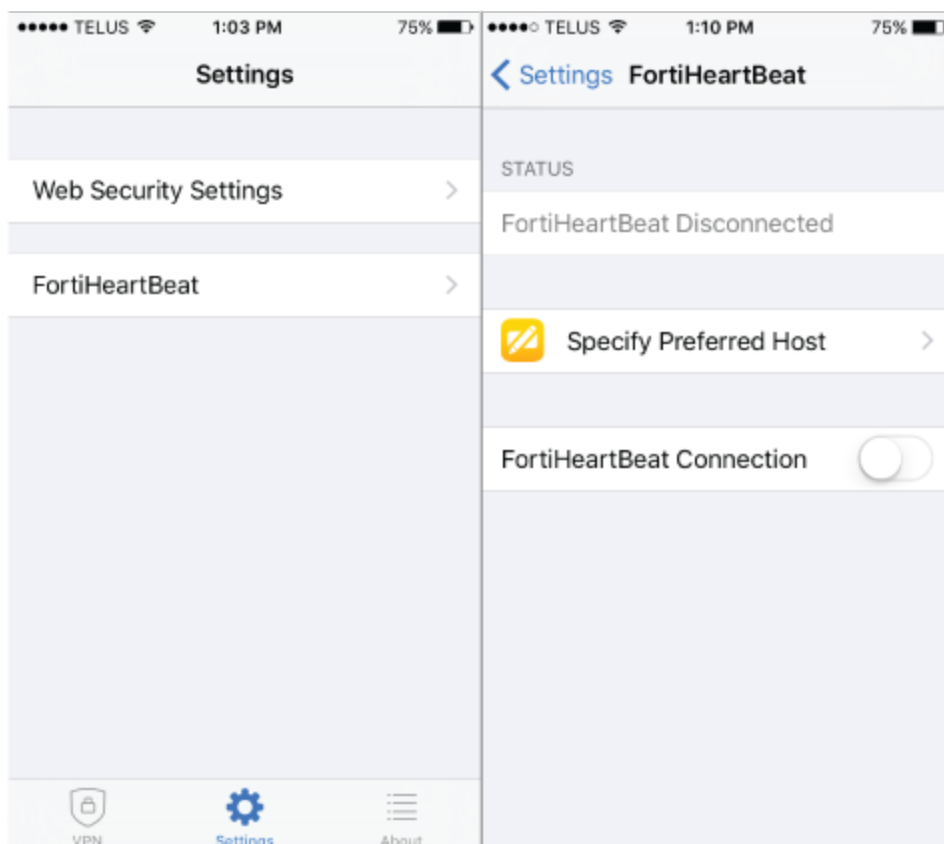


When a website is blocked, a restricted website error page will appear.

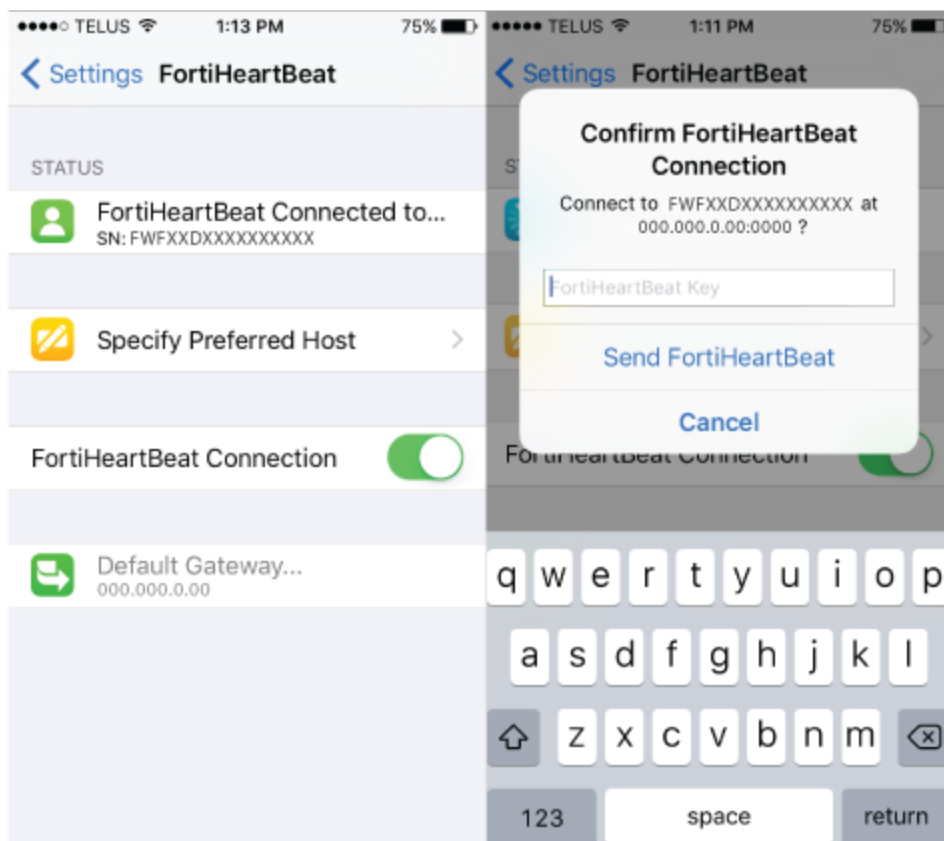
FortiHeartBeat

To configure the FortiHeartBeat settings:

1. Tap *Settings* at the bottom of the screen.
2. Tap *FortiHeartBeat*.



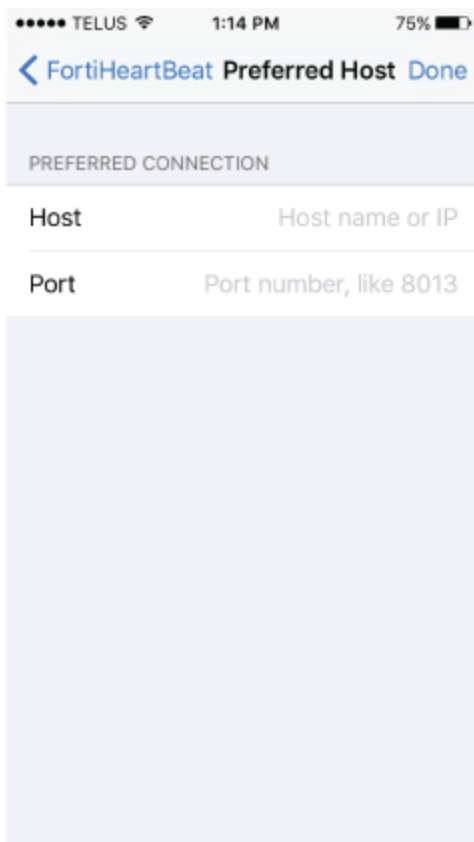
3. Enable *FortiHeartBeat* by swiping right.
When FortiClient detects a FortiHeartBeat server, a confirmation pop up window will appear.



4. Tap *Send FortiHeartBeat* to connect to the FortiHeartBeat server.

To specify a FortiHeartBeat server:

1. Tap *Specify Preferred Host*.



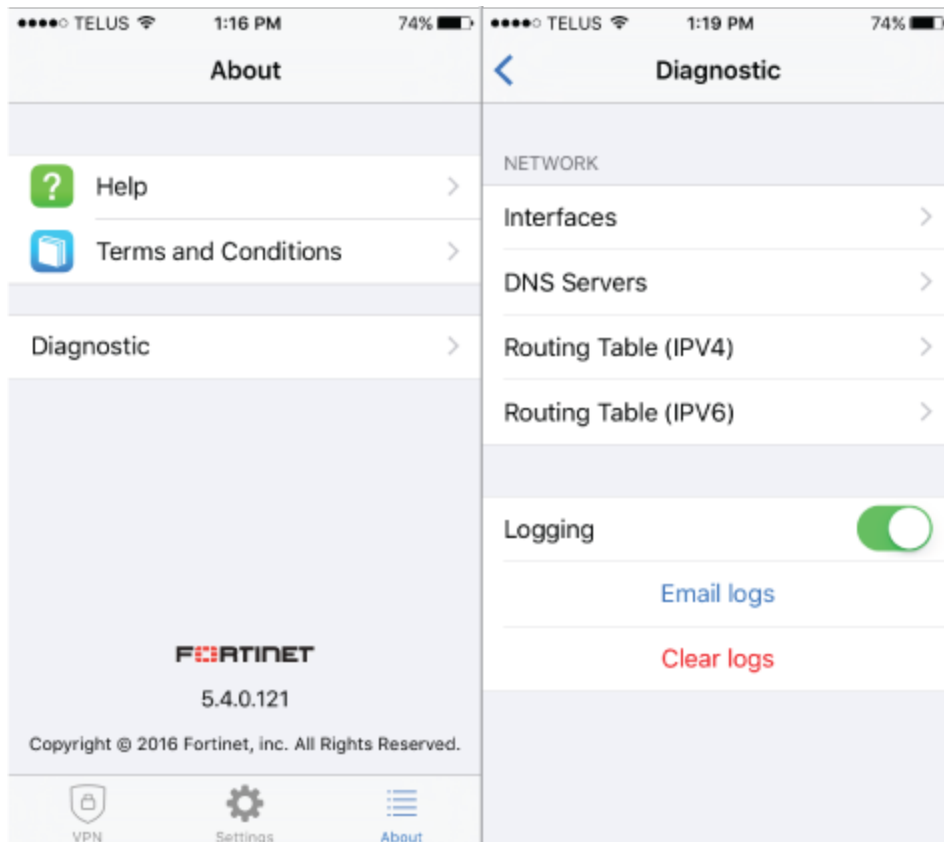
The screenshot shows an iPhone screen with the status bar at the top displaying 'TELUS', signal strength, time '1:14 PM', and battery '75%'. The app title bar is blue with a back arrow, 'FortiHeartBeat Preferred Host', and a 'Done' button. Below the title bar is a light blue header with the text 'PREFERRED CONNECTION'. The main content area has two input fields: 'Host' with the placeholder text 'Host name or IP' and 'Port' with the placeholder text 'Port number, like 8013'. Below these fields is a large, empty light blue rectangular box.

2. Enter *Host* and *Port*.
3. Tap *Done*.

Logs

You can email FortiClient iOS logs to Fortinet.

To email logs to Fortinet:



1. Tap *About* at the bottom of the screen.
2. Tap *Diagnostic*.
3. Swipe right to enable *Logging*.
4. Tap *Email Logs*.



FORTINET®

High Performance Network Security



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.